

PURPOSE

The Michigan Department of Health and Human Services (MDHHS) inventories, reviews and monitors third party risks and controls to ensure compliance with applicable laws, rules, regulations, and contract provisions.

INVENTORY

Bureau of Grants and Purchasing (BGP) will:

Bureau of Grants and Purchasing assesses all contracts and updates the financial Service Organization (SO) inventory on an annual basis. BGP assesses and updates the IT, cybersecurity, and other SO inventory during even numbered years. BGP uses guidance from the Financial Management Guide (FMG) to determine which contractors meet the definition of a SO. BGP sends the updated Inventory Worksheet to the MDHHS Internal Control Officer (ICO) within Bureau of Audit (BOA) for approval. The BOA ICO documents approval to BGP via email.

During August of each year, BGP distributes the SO Risk Assessment worksheet to each program area with a SO classified as financial. The Service Organization Risk Assessment worksheet is used to determine if a third-party assurance report is necessary to achieve the appropriate assurances on risks associated with SO services.

Programs will:

The Program area designee must contact Compliance for assistance in completing the SO Risk Assessment Worksheet to determine if a System and Organization Controls (SOC) report is required for the vendor and any of the vendor's subservice organizations. The program area designee submits completed SO Risk Assessment Worksheets to BGP.

BGP will:

BGP collects and sends all SO Risk Assessment Worksheets to the BOA Internal Control Evaluation (ICE) designee.

Bureau of Audit (BOA) will:

The BOA ICE designee reviews the worksheets for completeness.

Annually, by September 30th the BOA ICE designee submits the SO Inventory Worksheet and SO Risk Assessment Worksheets for financial reporting State of Michigan (SOM Annual Comprehensive Financial Report (ACFR)) related SOs to Office of Internal Audit Services (OIAS).

The separate inventory of material SOs to the department in IT, cybersecurity, and other areas is submitted to OIAS during even numbered years, by September 30th.

REPORT REVIEW

BOA will:

Bureau of Audit will utilize the 9/30/23 SO Inventory Worksheet that BGP provides to create and maintain a tracking sheet for the SOC reports, Bridge Letters, and SOC report reviews needed for the financial SOs that are material to the ACFR to help ensure timely receipt.

Beginning in FY24, BOA will request the SOC reports and Bridge letters from Programs starting in October. (Program area designees are responsible for contacting the SO to obtain the required SOC reports and Bridge letters, if applicable).

Starting with the 9/30/24 SO Inventory Worksheet, BOA will provide BGP with the following information to complete the annual SO Inventory Worksheet: (1) Date of Last Third-Party Assurance Report (if available) and (2) Reporting Period of Last Third-Party Assurance Report.

BOA will follow-up with Program designees to help ensure SOC reports and Bridge letters are obtained timely. Once received, BOA will maintain copies of the SOC reports and Bridge letters.

Programs and BOA will:

Each Program area designee is responsible for completing the SOC Report Review Template within 30 days of receipt of the SOC report from the SO. Compliance and BOA will perform a consulting role for SOC reports that are classified as financial and have a material impact on the ACFR.

The Program area designee must consult with Compliance on the technical portions of the SOC report review, including whether the scope of the SOC report covers the relevant systems that have

been outsourced to the SO, the determination of whether to obtain and review SOC reports for carved out subservice organizations, and the evaluation of any deviations or exceptions for a SOC report that does not have an unqualified opinion.

The Program area designee must consult with BOA on the complementary user entity control consideration portion of the SOC report review. The Program area is responsible for ensuring proper complementary user entity controls are in place during the scope of the SOC review. BOA will help ensure sufficient documentation is maintained at the program level to support that each control listed was in place.

The program designee will finalize the SOC report review by signing off on the evaluation completion and review sections of the SOC Report Review template and will send the completed template to BOA. The BOA ICO designee will send the final SOC Report Review template to OIAS after performing a final review of the template to make sure all required sections were completed.